IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No. : 10/786,224 Confirmation No. : 2832
First Named Inventor : Burkhard KUHLS
Filed : February 26, 2004
TC/A.U. : 2436
Examiner : Carlton Johnson
Docket No. : 080437.53236US
Title : Method for Providing Software to Be Used by a Control Unit …

PRE-APPEAL BRIEF REQUEST FOR REVIEW

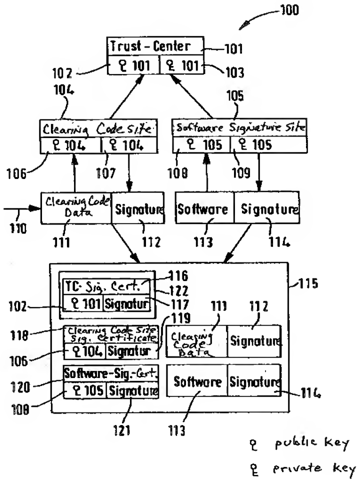
Sir:

Appellant requests review of the final rejection set forth in the Office Action dated December 19, 2011.

The rejection of claims 1, 4-9, and 12-19 for anticipation by Schmidt is improper and should be withdrawn. Due to the page limitations imposed on this Request, the discussion below focuses on why Schmidt does not anticipate claim 19. It should be recognized, however, the anticipation rejection based on Schmidt contains similar deficiencies with respect to the other rejected claims. As will be discussed in detail below, Appellant's claim 19 recites the storage of ***three*** different types of certificates each with distinct public keys, whereas Schmidt at best discloses ***two*** different types of certificates.

I. Appellant Discloses Distinct Certificates that Include Distinct Public Keys

Exemplary embodiments of the present invention employ a trust center 101, software signature site 105, clearing code site 106 and control unit 115 for the generation and verification of certification to control the exchange or alteration of software used by vehicle control units. Control unit 115 can store the following certificates:



1. T<u>rust center certificate 116</u> generated using secret key 103 of trust center 101 and including public key 101 and signature 117 generated using secret key 103;
2. <u>Clearing code site signature certificate 118</u> generated using public key 106 of clearing code site 104 and private key 103 of trust center 101;
3. <u>Software signature certificate 120</u> generated using private key 103 of trust center 101 and public key 108 of software signature site 105, and including public key 108 of software signature site 105, a signature 121 generated by trust center 101 and one or more validity restrictions.

Accordingly, each of these certificates 116, 118, and 120 are disclosed as distinct types of certificates.

II. Claim 19 Recites Three Distinct Certificates that Include Distinct Public Keys

Claim 19 recites a method of providing software for use by a control unit of a vehicle that involves storing the following three different types of certificates in the control unit:

1. A trust center certificate including a public key and a signature generated using a secret key of a trust center;
2. A clearing code site signature certificate including a second public key and a second signature; and
3. A software signature certificate including a third public key and a third signature.

By using different terms to characterize the different certificates claim 19 clearly requires that these three certificates be distinct types of certificates. Similarly, by referring to the public keys using different terms claim 19 clearly requires that the public keys of the distinct types of certificates be distinct types of public keys. This interpretation of the certificates and public keys is consistent with the specification.

III. Schmidt At Best Discloses Two Different Types of Certificate with the Same Type of Public Key

Schmidt's includes a detailed discussion of how to generate a single type of certificate. However, as will be discussed below in connection with the multiple certificate disclosures of Schmidt, it is assumed these disclosures involve two different types of certificates.

A. Schmidt's Detailed Discussion of Certificate Generation Involves a Single Type of Certificate

Referring to Figs. 3 and 4 of Schmidt (reproduced below),[1] a certificate holder 312, 400 (e.g., a dealer or shop) generates its own private/public key pair 314, 316, and sends its public key 316 to trust center 404. Trust center 404 generates certificate 318, 406, which is signed by its own private key 304 and sends the signed certificate 318, 406 to the certificate holder 312, 400. Although Schmidt does not detail how the certificate holder's public key 316 is placed in the certificate 318, 406, it appears that this is also performed by trust center 404. Certificate holder 312, 400 can then use the certificate to sign software 408, which can then be imported into the vehicle control unit.

[1] Fig. 3 is annotated to include text labels.

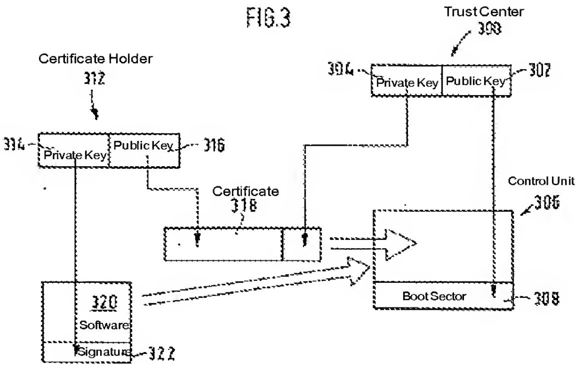


FIG.3

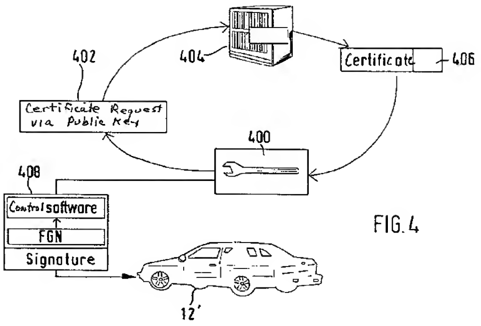


FIG. 4

As is clear from the disclosure of Schmidt, certificate 318 of Fig. 3 is the same type of certificate as certificate 406 of Fig. 4. Thus, Schmidt discloses only a single type of certificate, which is used for allowing authorized parties to generate software that can be installed in vehicle control units.[2]

B. Schmidt's Disclosure of Multiple Certificates At Best Involves Two Types of Certificates

Schmidt discusses the use of multiple certificates in paragraphs 0017-0018 and in paragraph 0050. Paragraphs 0017-0018 disclose using multiple certificates jointly so that the signature of the first certificate is checked using the key filed in the control unit, the signatures of the subsequent certificates are checked using the key contained in the previously accepted certificate, and the signature of the software is checked using the key in the last certificate. In this multiple certificate scenario it appears that all of the certificates are the same type of certificate and use the same type of public key. Assuming, *arguendo*, Schmidt is interpreted so that the last certificate that is used to check the signature of the software is a software signature certificate and the previously used certificates are different from the last certificate, this would at best result in ***two*** different types of certificates, whereas Appellant's claim 19 requires ***three*** different types of certificates.[3] Given the overall disclosure of Schmidt, however, it appears that these certificates are all generated in the same manner using the technique illustrated in Figs. 3 and 4, and thus when considered as a whole, Schmidt actually discloses only a single type of certificate.

Paragraph 0050 discusses avoiding all software volumes being signed by a single party by using "several decentralized authorized parties –so-called certificate holders- (for example, dealers)." In this scenario all certificate holders would have the same type of

[2] Paragraph 0050.

[3] This should not be interpreted as an acknowledgement that Schmidt discloses two different types of certificates, but instead is intended to address expected examiner arguments regarding the disclosure of Schmidt.

certificate so each could sign software volumes. This is true regardless of the fact that the public keys themselves would be different because the public keys would be the same type of public keys, namely dealer public keys.

Because Schmidt's disclosure of multiple certificates at best involves two types of certificates, Schmidt does not disclose the three types of certificates required by claim 19.

IV. The Rejection of Claim 19 Clearly Relies on the Same Type of Certificate and the Same Type of Public Key in Schmidt

The final Office Action provides an identical explanation of how Schmidt discloses the storage of the three distinct certificates recited in claim 19 – "see Schmidt paragraph [0060], lines 1-4; generate certificate, signs it and sends it back to certificate holder where it remains (stored)."[4] Although this accurately characterizes the cited portion of Schmidt, it ignores the language of claim 19. First, claim 19 recites that the three distinct certificates are stored in the control unit. In contrast, certificate holder 400 in Schmidt is not the control unit of the vehicle 12', rather Schmidt discloses that certificate holder 400 is a shop.[5] Thus, the cited section of Schmidt discloses the same type of certificate, namely a shop certificate that would at best include a public key of a shop. In contrast, claim 19 recites three different types of certificates with three distinct types of public keys. Accordingly, the shop certificate disclosed in paragraph 0060 of Schmidt is a single type of certificate with single type of key.

V. Generating the Same Type of Certificate for Different Entities Does not Disclose the Three Different Certificates of Claim 19

The Advisory Action states that the certificates of Schmidt "are not the same since each certificate is used to authorize a different entity." Authorizing different entities using different certificates does not change the fact that the purpose of all of these certificates is the same – to allow only authorized entities to load authorized software into a control unit. Thus, these different entities all have the same type of certificate, just with different public keys for the different authorized entities.

VI. The Advisory Action Improperly Equates a Trust Center and Vehicle Control Unit

The Advisory Action provides the following explanation of how Schmidt discloses that a trust center is the same as a vehicle control unit:

> See Schmidt paragraph [0059], lines 6-10: generates key pair and sends public key with certificate request; paragraph [0060], lines 1-4: trust center (control unit) generates certificate, signs by means of

[4] Final Office Action at pages 13 and 14.

[5] See, for example, paragraph 0059.

> secret key (trust center) and sends to certificate holder; paragraph [0012], lines 6-9: trust center analogous to vehicle, control unit.

None of these cited sections of Schmidt disclose that the trust center can be the vehicle control unit, and this position is contrary to the figures that clearly illustrate that the trust center is distinct from the vehicle control unit. This is also contrary to the entire purpose of Schmidt, which is to provide an independent trust center to control authorized installation of software in control units. If, as the Advisory Action proposes, the functions of the trust center were incorporated into the control unit of the vehicle, then Schmidt would not have the necessary independent trust center to control this authorized software installation.

VII. The Rejection Uses an Inconsistent Interpretation of the Term "Certificate"

The Advisory Action appears to take the position that in some cases a certificate is a certificate and in other cases a secret key by itself is a certificate. For example, the Advisory Action states:

> Schmidt discloses a ***certificate*** used to authorize the usage of software (software signature certificate). Schmidt discloses a ***certificate*** that indicates a specific control unit (clearing code site certificate). And, Schmidt discloses a ***secret key*** of a control unit for a vehicle (trust center certificate)."[6]

Interpreting a secret key by itself as a certificate ignores Appellant's specification, as well as the express disclosure of Schmidt. Although Schmidt discloses that the private key of the trust center 300 is used to sign the single type of certificate (see Fig. 3), Schmidt does not disclose that the private key by itself is a certificate. The Advisory Action does not explain why in some cases a certificate is a certificate and in others a private key by itself is a certificate. Thus, there is insufficient evidence in the record for the Board of Appeals to uphold a rejection that relies upon a private key as a certificate when Appellant's specification and Schmidt both do not disclose that a private key by itself is a certificate.

VIII. Conclusion

For the reasons set forth above, it is respectfully submitted that the rejection of claim 19 for anticipation by Schmidt should be withdrawn. The other pending claims are patentably distinguishable for similar reasons.

Respectfully submitted,

April 18, 2012

/Stephen W. Palan, Reg. No. 43,420/
Stephen W. Palan
Registration No. 43,420

[6] Advisory Action, page 2. (Emphasis added).